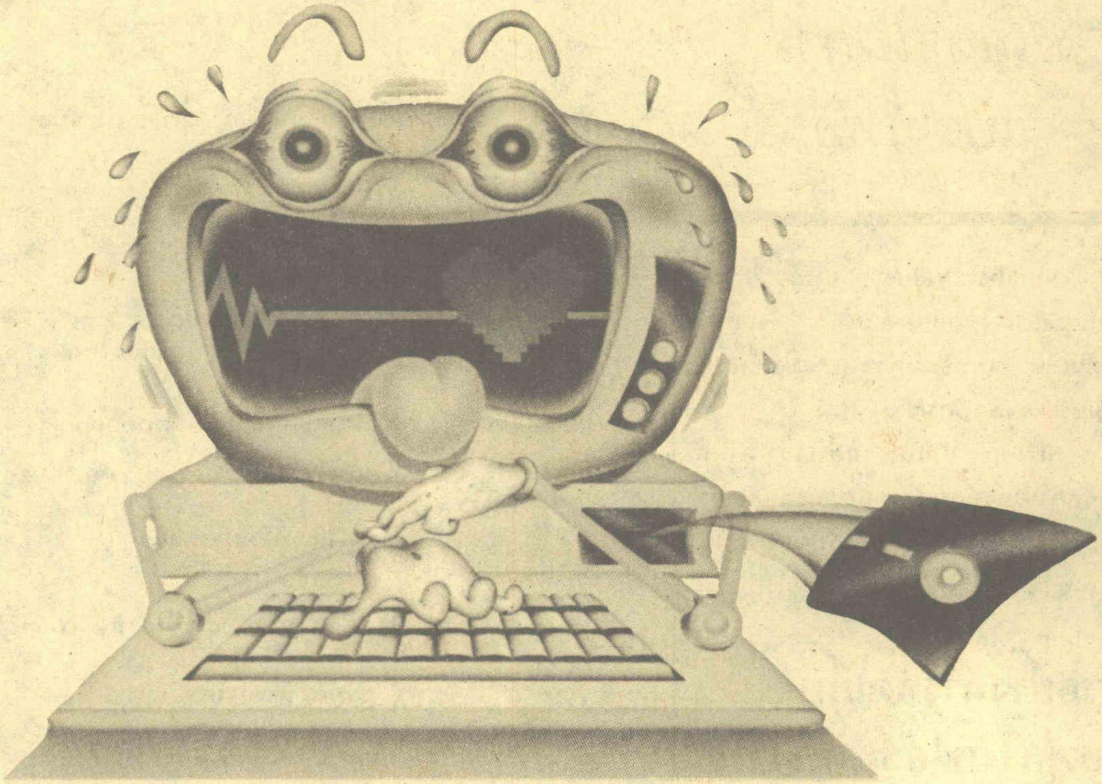
ประสบการณ์ไวรัส



กิตติรัตน์ มโนสุทธิ

ตอนแรกที่ผมได้ทราบข่าวคราวของเจ้าตัวบ่อนทำลายนี้ ผมก็ไม่ค่อยอยากจะเชื่อเท่าไหร่นัก เพราะรู้สึกว่ามันพิสดารเหลือเกิน จนกระทั่งเป็นข่าวใหญ่ขึ้นมานั่นแหละครับถึงเริ่มเชื่อ แต่พอไปเล่าให้ใคร ๆ ฟังว่าไวรัสคืออะไร ปรากฏว่าผมโดนหาว่าบ้า เฮ้อ!

เมื่อเวลาล่วงเลยมาอีกสักหน่อย จนมันแพร่เข้ามาใกล้ตัวผมทุกที ก็เลยเกิดความอยากลองดีกับมันสักตั้ง ผมเลยไปขอยืมแผ่นซิสเต็มส์ ที่มีเจ้าตัวกินแผ่นนี้แหละครับมาจากเพื่อน (ซึ่งก็โดนไปเรียบร้อยแล้ว) มาลองแกะดูว่ามันทำอะไรได้บ้าง ผลสรุปเท่าที่ผมโดนก็คือ

1. ถ้าไม่ได้เอาแผ่นไวรัสมาบูตเครื่อง ก็เป็นปกติธรรมดา ผมเอาแผ่นไวรัสไว้ที่ไดรฟ์ B: แล้วเอาโปรแกรม symdeb (โปรแกรมดีบักชนิดหนึ่ง ซึ่งคงรู้จักกันดีอยู่แล้ว) ไว้ที่ไดรฟ์ A: เพื่อดูที่บูตเรคอร์ดของแผ่นไวรัส ก็ปรากฏข้อความดังรูปที่ 1 นี่ก็แปลว่าเจ้าตัวดีนี่ไปจัดการโปรแกรมบูตของแผ่นเข้าให้แล้ว จากนั้นผมก็มาแกะโปรแกรมบูตของมันดู ก็จะได้ตามรูปที่ 2

รูปที่ 1 ข้อความที่ปรากฏในส่วนบูตเรคอร์ดจากแผ่นไวรัส

```
A>symdeb
Microsoft (R) Symbolic Debug Utility  Version 4.00
Copyright (C) Microsoft Corp 1984, 1985.  All rights reserved.

Processor is [8086]
-l cs:100 1 0 1
-d100 300
1E9C:0100  FA E9 4A 01 34 12 01 02-0F 00 01 00 00 00 00 00  ziJ.4...........
1E9C:0110  57 65 6C 63 6F 6D 65 20-74 6F 20 74 68 65 20 20  Welcome to the
1E9C:0120  44 75 6E 67 65 6F 6E 20-20 20 20 20 20 20 20 20  Dungeon
1E9C:0130  28 63 29 20 31 39 38 36-20 42 72 61 69 6E 17 26  (c) 1986 Brain.&
1E9C:0140  20 41 6D 6A 61 64 73 20-28 70 76 74 29 20 4C 74   Amjads (pvt) Lt
1E9C:0150  64 20 20 20 56 49 52 55-53 5F 53 48 4F 45 20 20  d   VIRUS_SHOE
1E9C:0160  52 45 43 4F 52 44 20 20-20 76 39 2E 30 20 20 20  RECORD   v9.0
1E9C:0170  44 65 64 69 63 61 74 65-64 20 74 6F 20 74 68 65  Dedicated to the
1E9C:0180  20 64 79 6E 61 6D 69 63-20 6D 65 6D 6F 72 69 65   dynamic memorie
1E9C:0190  73 20 6F 66 20 6D 69 6C-6C 69 6F 6E 73 20 6F 66  s of millions of
1E9C:01A0  20 76 69 72 75 73 20 77-68 6F 20 61 72 65 20 6E   virus who are n
1E9C:01B0  6F 20 6C 6F 6E 67 65 72-20 77 69 74 68 20 75 73  o longer with us
1E9C:01C0  20 74 6F 64 61 79 20 2D-20 54 68 61 6E 6B 73 20   today - Thanks
1E9C:01D0  47 4F 4F 44 4E 45 53 53-21 21 20 20 20 20 20 20  GOODNESS!!
1E9C:01E0  20 42 45 57 41 52 45 20-4F 46 20 54 48 45 20 65   BEWARE OF THE e
1E9C:01F0  72 2E 2E 56 49 52 55 53-20 20 3A 20 5C 74 68 69  r..VIRUS  : \thi
1E9C:0200  73 20 70 72 6F 67 72 61-6D 20 69 73 20 63 61 74  s program is cat
1E9C:0210  63 68 69 6E 67 20 20 20-20 20 20 70 72 6F 67 72  ching      progr
1E9C:0220  61 6D 20 66 6F 6C 6C 6F-77 73 20 61 66 74 65 72  am follows after
1E9C:0230  20 74 68 65 73 65 20 6D-65 73 73 65 67 65 73 2E   these messeges.
1E9C:0240  2E 2E 2E 2E 20 24 23 40-25 24 40 21 21 20 8C C8  .... $#@%$@!! .H
1E9C:0250  8E D8 8E D0 BC 00 F0 FB-A0 06 7C A2 09 7C 8B 0E  .X.P<.p{ .¦".¦..
1E9C:0260  07 7C 89 0E 0A 7C E8 57-00 B9 05 00 BB 00 7E E8  .¦...¦hW.9..;.~h
1E9C:0270  2A 00 E8 4B 00 81 C3 00-02 E2 F4 A1 13 04 2D 07  *.hK..C..bt!..-.
1E9C:0280  00 A3 13 04 B1 06 D3 E0-8E C0 BE 00 7C BF 00 00  .#..1.S`.@>.¦?..
1E9C:0290  B9 04 10 FC F3 A4 06 B8-00 02 50 CB 51 53 B9 04  9..¦s$.8..PKQS9.
1E9C:02A0  00 51 8A 36 09 7C B2 00-8B 0E 0A 7C B8 01 02 CD  .Q.6.¦2....¦8..M
1E9C:02B0  13 73 09 B4 00 CD 13 59-E2 E7 CD 18 59 5B 59 C3  .s.4.M.YbgM.Y[YC
1E9C:02C0  A0 0A 7C FE C0 A2 0A 7C-3C 0A 75 1A C6 06 0A 7C   .¦~@".¦<.u.F..¦
1E9C:02D0  01 A0 09 7C FE C0 A2 09-7C 3C 02 75 09 C6 06 09  . .¦~@".¦<.u.F..
1E9C:02E0  7C 00 FE 06 0B 7C C3 00-00 00 00 32 E3 23 4D 59  ¦.~..¦C....2c#MY
1E9C:02F0  F4 A1 82 BC C3 12 00 7E-12 CD 21 A2 3C 5F 0C 05  t!.<C..~.M!"<_..
1E9C:0300  C1                                               A
-q

A>
```

รูปที่ 2 โปรแกรมบูตของแผ่นไวรัส

```
A>symdeb
Microsoft (R) Symbolic Debug Utility  Version 4.00
Copyright (C) Microsoft Corp 1984, 1985.  All rights reserved.

Processor is [8086]
-l cs:100 1 0 1
-u100 104
13EE:0100 FA            CLI
13EE:0101 E94A01        JMP     024E
13EE:0104 3412          XOR     AL,12
-
-u24e 300
13EE:024E 8CC8          MOV     AX,CS
13EE:0250 8ED8          MOV     DS,AX
```

```
13EE:0252 8ED0          MOV     SS,AX
13EE:0254 BC00F0        MOV     SP,F000
13EE:0257 FB            STI
13EE:0258 A0067C        MOV     AL,[7C06]
13EE:025B A2097C        MOV     [7C09],AL
13EE:025E 8B0E077C      MOV     CX,[7C07]
13EE:0262 890E0A7C      MOV     [7C0A],CX
13EE:0266 E85700        CALL    02C0
13EE:0269 B90500        MOV     CX,0005
13EE:026C BB007E        MOV     BX,7E00
13EE:026F E82A00        CALL    029C
13EE:0272 E84B00        CALL    02C0
13EE:0275 81C30002      ADD     BX,0200
13EE:0279 E2F4          LOOP    026F
13EE:027B A11304        MOV     AX,[0413]
13EE:027E 2D0700        SUB     AX,0007
13EE:0281 A31304        MOV     [0413],AX
13EE:0284 B106          MOV     CL,06
13EE:0286 D3E0          SHL     AX,CL
13EE:0288 8EC0          MOV     ES,AX
13EE:028A BE007C        MOV     SI,7C00
13EE:028D BF0000        MOV     DI,0000
13EE:0290 B90410        MOV     CX,1004
13EE:0293 FC            CLD
13EE:0294 F3            REPZ
13EE:0295 A4            MOVSB
13EE:0296 06            PUSH    ES
13EE:0297 B80002        MOV     AX,0200
13EE:029A 50            PUSH    AX
13EE:029B CB            RETF
13EE:029C 51            PUSH    CX
13EE:029D 53            PUSH    BX
13EE:029E B90400        MOV     CX,0004
13EE:02A1 51            PUSH    CX
13EE:02A2 8A36097C      MOV     DH,[7C09]
13EE:02A6 B200          MOV     DL,00
13EE:02A8 8B0E0A7C      MOV     CX,[7C0A]
13EE:02AC B80102        MOV     AX,0201
13EE:02AF CD13          INT     13
13EE:02B1 7309          JNB     02BC
13EE:02B3 B400          MOV     AH,00
13EE:02B5 CD13          INT     13
13EE:02B7 59            POP     CX
13EE:02B8 E2E7          LOOP    02A1
13EE:02BA CD18          INT     18
13EE:02BC 59            POP     CX
13EE:02BD 5B            POP     BX
13EE:02BE 59            POP     CX
13EE:02BF C3            RET
13EE:02C0 A00A7C        MOV     AL,[7C0A]
13EE:02C3 FEC0          INC     AL
13EE:02C5 A20A7C        MOV     [7C0A],AL
13EE:02C8 3C0A          CMP     AL,0A
13EE:02CA 751A          JNZ     02E6
13EE:02CC C6060A7C01    MOV     Byte Ptr [7C0A],01
13EE:02D1 A0097C        MOV     AL,[7C09]
13EE:02D4 FEC0          INC     AL
13EE:02D6 A2097C        MOV     [7C09],AL
13EE:02D9 3C02          CMP     AL,02
13EE:02DB 7509          JNZ     02E6
13EE:02DD C606097C00    MOV     Byte Ptr [7C09],00
13EE:02E2 FE060B7C      INC     Byte Ptr [7C0B]
13EE:02E6 C3            RET
13EE:02E7 0000          ADD     [BX+SI],AL
13EE:02E9 0000          ADD     [BX+SI],AL
13EE:02EB 32E3          XOR     AH,BL
13EE:02ED 234D59        AND     CX,[DI+59]
13EE:02F0 F4            HLT
13EE:02F1 A182BC        MOV     AX,[BC82]
13EE:02F4 C3            RET
13EE:02F5 1200          ADC     AL,[BX+SI]
13EE:02F7 7E12          JLE     030B
13EE:02F9 CD21          INT     21
13EE:02FB A23C5F        MOV     [5F3C],AL
13EE:02FE 0C05          OR      AL,05
13EE:0300 0000          ADD     [BX+SI],AL
-q

A>
A>
```

VIRUS! Boot Routine

ลองดูที่รูปที่ 2 ดูนะครับ ที่ออฟเซตแอดเดรส 0269-0279 (เซกเมนต์-แอดเดรสไม่ต้องไปสนใจมันหรอกครับ เพราะเวลาบูตเครื่อง บูตสเตรปรูทีนในรอมจะจัดการโหลดโปรแกรมบูตจากแผ่นดิสก์ ไปไว้ที่เอปโซลุตแอดเดรส 07C00h แล้วจึงส่งผ่านการควบคุมไปยังรูทีนจากแผ่นดิสก์) จะเห็นว่ามันทำการโหลดข้อมูลจากแผ่นลงมา ยังแอดเดรสที่กำหนดไว้คือ ES:BX และที่แอดเดรส 027B-0281 เป็นการเปลี่ยนข้อมูลแสดงขนาดของหน่วยความจำระบบจากเดิมลงมาอีก 7 กิโลไบต์ (ที่ตำแหน่ง 0413h เป็นตำแหน่งเก็บขนาดของหน่วยความจำระบบ ซึ่งส่วนนี้อยู่ใน BIOS Data Area) ตรงนี้แหละครับเป็นตัวแสดงว่า ไวรัสมันจะไปกันเนื้อที่หน่วยความจำของเราไว้ 7 กิโลไบต์ เพื่ออะไรนั้นผมกำลังหาอยู่ แต่ก็เดาว่าคงจะเป็นการเก็บตัวมันลงไปนั่นเอง

จากนั้น ที่แอดเดรส 0284-0295 เป็นการเคลื่อนย้ายข้อมูลจากหน่วยความจำตำแหน่งที่ชี้โดย DS:SI ไปยังตำแหน่งที่ชี้โดย ES:DI เอาละครับ ลองไล่โปรแกรมกันดูเองก็แล้วกัน เพื่อความมันบนใบหน้า!

2. ขั้นต่อไปผมฟอร์แมตแผ่นดิสก์ไว้ 1 แผ่น โดยไม่ได้ใส่ option/s คือไม่ได้ใส่ซิสเต็มส์ลงไปด้วย แล้วก็เอาแผ่นไวรัสมาบูตเครื่อง โดยแผ่นใหม่ของผมนี้เอาไว้ที่ไดร์ฟ B: เมื่อบูตเครื่องคุณจะสังเกตได้อย่างหนึ่งเลยว่า มันจะใช้เวลานานกว่าปกติ เมื่อเครื่องขึ้น A> แล้ว ผมก็ลอง dir b: ดู ปรากฏว่านอกจากมันจะอ่านแผ่นอย่างเดียวแล้ว ยังกลับเขียนอะไรต่ออะไรลงไปอีก ที่เห็นชัดคือ มันจะไปเปลี่ยน Vol. label ของแผ่นให้เป็นตามรูปที่ 3 (กลายเป็น (c) Brain) อันนี้ไม่แน่นอนครับ เพราะ

รูปที่ 3 อาการอย่างหนึ่งของแผ่นที่ถูกไวรัสคุกคาม เมื่อใช้คำสั่ง DIR

```
 Volume in drive B is  (c) Brain
 Directory of  B:\

.  IBMBIO   COM    IBMDOS   COM    COMMAND  COM    VIRUS    TXT    VIRUS    ASM
 PROTECT  COM    BOOTSEC  ASM    BOOTSEC  TXT    1        BAT    SEARCH   COM
        10 File(s)    211968 bytes free
```

บางทีมันก็ไม่เปลี่ยน แต่ที่ผมเจอทุกครั้งคือ มันจะกินแผ่นของเราไป 3 คลัสเตอร์

3. ถ้าเราฟอร์แมตแผ่นด้วย option /s แล้วลองบูตด้วยแผ่นไวรัสนั่นแหละ พอ dir B: ดูเท่านั้นแหละ เรียบร้อย โรงเรียนไวรัส ซิสเต็มส์ของเราบนแผ่นใหม่ก็จะนอกใจคุณทันที เพราะมันจะกลายเป็นพวกไวรัสไปเลย (ลองดูได้ โดยการเอาแผ่นนี้ไปบูต จะมีไวรัสหล่นลงไปในเครื่องของคุณด้วย)

จากทั้งหมดนี้ยังไม่ครบถ้วนทุกอาการนะครับ เพราะบางอาการผมก็ไม่สามารถจะรายงานออกมาเป็นถ้อยคำได้ คุณต้องลองเอาเอง (แต่ว่า อยากจะเสี่ยงเหรอ!) ผมมีข้อแนะนำบางอย่างให้กับผู้เข้ามาใหม่ในโลกแห่งไวรัส (ความจริงผมก็เพิ่งจะเริ่มเหมือนกันแหละ) คือว่า ถ้าคุณอยากจะเล่นกับมัน คุณก็ต้องมีอาวุธคู่มือใช่มั้ยครับ เช่น พวก Norton Utility, PC Tools, Debug อะไรทำนองนี้แหละ แต่คุณอย่าลืมแปะ write protect เข้าไปทุกแผ่นนะครับ ไม่งั้นมันอาจจะออกไปเพ่นพ่านเต็มบ้านคุณก็ได้ เดี๋ยวจะหาว่าไม่เตือน

คุณคงจำได้ว่า ในหัวข้อที่ 2 เราทราบแล้วว่า มันจะไปจัดการเปลี่ยนขนาดของหน่วยความจำระบบให้ลดลงไป 7 กิโลไบต์ ตรงจุดนี้แหละครับ ที่เราสามารถจะเช็คได้ว่าตอนนี้ ระบบของคุณติดเชื้อเข้าให้หรือยัง โดยการอ่านขนาดหน่วยความจำจากดอสหรือจะไปอ่านที่ตรงนั้นโดยตรงก็ได้ การเช็คขนาดหน่วยความจำนี้ คุณอาจจะเช็คได้ตั้งหลายวิธี เช่นจาก SI (System Information) ของ Norton หรือจาก

รูปที่ 4 ผลของการทำงานโปรแกรมเช็คขนาดหน่วยความจำระบบ

```
Segments and Groups:

                N a m e                 Length   Align   Combine Class

CODE . . . . . . . . . . . . .          0336    PARA    PUBLIC  'CODE

Symbols:

                N a m e                 Type     Value   Attr

AUTHOR . . . . . . . . . . . .          L BYTE  0118    CODE

BEGIN . . . . . . . . . . . .           L NEAR  0100    CODE

COPYRIGHT . . . . . . . . . .           L BYTE  0103    CODE

DATE . . . . . . . . . . . . .          L BYTE  012D    CODE

OK . . . . . . . . . . . . . .          L NEAR  0322    CODE

QUIT . . . . . . . . . . . . .          L NEAR  032B    CODE

SEARCH . . . . . . . . . . . .          N PROC  02F0    CODE    Length = 003F
STARTTEXT . . . . . . . . . .           L BYTE  0294    CODE

TEXT1 . . . . . . . . . . . .           L BYTE  0146    CODE
TEXT2 . . . . . . . . . . . .           L BYTE  01A9    CODE
TEXT3 . . . . . . . . . . . .           L BYTE  0257    CODE
TIME . . . . . . . . . . . . .          L BYTE  013B    CODE

UNKNOWN . . . . . . . . . . .           L NEAR  030C    CODE

VIRUS . . . . . . . . . . . .           L NEAR  0317    CODE

WRITE . . . . . . . . . . . .           N PROC  032F    CODE    Length = 0007

@FILENAME . . . . . . . . . .           TEXT  search


     79 Source  Lines
     79 Total   Lines
     18 Symbols

  51082 + 393942 Bytes symbol space free

      0 Warning Errors
      0 Severe  Errors
```

รูปที่ 5 โปรแกรมเช็คขนาดหน่วยความจำระบบ

```
                                page 60,132
0000                            code        segment  para public 'code'
                                            assume   cs:code

0100                                        org      100h
0100  E9 02F0 R                 begin:      jmp      search

                                ;
                                ; Data area
                                ;

0103  57 41 54 43 4F 4D 21      Copyright   db  'WATCOM! International'
      20 49 6E 74 65 72 6E
      61 74 69 6F 6E 61 6C
0118  4D 72 2E 4B 69 74 74      Author      db  'Mr.Kittiwat Manosuthi'
      69 77 61 74 20 4D 61
      6E 6F 73 75 74 68 69
012D  57 65 64 20 20 35 2D      Date        db  'Wed  5-04-1988'
      30 34 2D 31 39 38 38
013B  32 30 3A 35 33 3A 33      Time        db  '20:53:37.57'
      37 2E 35 37

0146  4D 65 6D 6F 72 79 20      Text1       db  'Memory at BIOS data area not equal to 640K Bytes..',13,10
      61 74 20 42 49 4F 53
      20 64 61 74 61 20 61
      72 65 61 20 6E 6F 74
      20 65 71 75 61 6C 20
      74 6F 20 36 34 30 4B
      20 42 79 74 65 73 2E
      2E 0D 0A
017A  42 75 74 20 74 68 65              db  'But there is no Known-VIRUS in your system.',13,10,10,'$'
      72 65 20 69 73 20 6E
      6F 20 4B 6E 6F 77 6E
      2D 56 49 52 55 53 20
      69 6E 20 79 6F 75 72
      20 73 79 73 74 65 6D
      2E 0D 0A 0A 24

01A9  4F 68 21 20 47 6F 64      Text2       db  'Oh! God. I found the Known-VIRUS in your system.',13,10
      2E 20 49 20 66 6F 75
      6E 64 20 74 68 65 20
      4B 6E 6F 77 6E 2D 56
      49 52 55 53 20 69 6E
      20 79 6F 75 72 20 73
      79 73 74 65 6D 2E 0D
      0A
01DB  50 6C 65 61 73 65 20              db  'Please turn your system off, now!',13,10
      74 75 72 6E 20 79 6F
      75 72 20 73 79 73 74
      65 6D 20 6F 66 66 2C
      20 6E 6F 77 21 0D 0A
01FE  41 6E 64 20 72 65 62              db  'And reboot your system with another system diskette.',13,10
      6F 6F 74 20 79 6F 75
      72 20 73 79 73 74 65
      6D 20 77 69 74 68 20
      61 6E 6F 74 68 65 72
      20 73 79 73 74 65 6D
```

```
      20 64 69 73 6B 65 74
      74 65 2E 0D 0A
0234  46 6F 72 20 6D 6F 72              db  'For more information, see text.',13,10,10,'$'
      65 20 69 6E 66 6F 72
      6D 61 74 69 6F 6E 2C
      20 73 65 65 20 74 65
      78 74 2E 0D 0A 0A 24

0257  48 61 76 65 20 61 20        Text3       db  'Have a happy day!'
      68 61 70 70 79 20 64
      61 79 21
0268  20 54 68 65 72 65 20              db  ' There is no Known-VIRUS in your system.',13,10,10,'$'
      69 73 20 6E 6F 20 4B
      6E 6F 77 6E 2D 56 49
      52 55 53 20 69 6E 20
      79 6F 75 72 20 73 79
      73 74 65 6D 2E 0D 0A
      0A 24

0294  0D 0A 56 69 72 75 73        StartText   db  13,10,'Virus Searcher (R) Version 1.0',13,10
      20 53 65 61 72 63 68
      65 72 20 28 52 29 20
      56 65 72 73 69 6F 6E
      20 31 2E 30 0D 0A
02B6  43 6F 70 79 72 69 67              db  'Copyright (C) WATCOM! Int''l 1988. All rights reserved.',13,10,10,'$'
      68 74 20 28 43 29 20
      57 41 54 43 4F 4D 21
      20 49 6E 74 27 6C 20
      31 39 38 38 2E 20 41
      6C 6C 20 72 69 67 68
      74 73 20 72 65 73 65
      72 76 65 64 2E 0D 0A
      0A 24
```

```
                        ;-------------------------------------------------------
                        ; NOTE:: At memory location 04130h in BIOS data area, it
                        ;        contains size of system memory in K bytes.
                        ;-------------------------------------------------------

02F0                    SEARCH      proc    near
02F0  33 C0                         xor     ax,ax           ;reset AX
02F2  8E D8                         mov     ds,ax           ;DS=0000
02F4  A1 0413                       mov     ax,ds:[0413h]   ;get size of mem from bios data area
02F7  8C CA                         mov     dx,cs           ;DX=CS
02F9  8E DA                         mov     ds,dx           ;DS=CS
02FB  8D 16 0294 R                  lea     dx,StartText    ;print version
02FF  E8 032F R                     call    write
0302  3D 0279                       cmp     ax,633          ;VIRUS eats 7K Bytes from 640K?
0305  74 10                         je      short virus     ;if equal, sorry to you
0307  3D 0280                       cmp     ax,640          ;is system memory=640K Bytes?
030A  74 16                         je      short ok        ;yes,quit with 0
030C  8D 16 0146 R          UnKnown:lea     dx,text1        ;memory not equal to 640K
0310  E8 032F R                     call    write           ; so, display text
0313  B0 01                         mov     al,1            ; and quit with return code 1
0315  EB 14                         jmp     short quit

0317  8D 16 01A9 R          Virus:  lea     dx,text2        ;ther is the VIRUS in your system
031B  E8 032F R                     call    write           ; so,display alert text
031E  B0 FF                         mov     al,0FFh         ; and quit with return code FFh
0320  EB 09                         jmp     short quit
```

```
0322  8D 16 0257 R          Ok:     lea     dx,text3        ;your system is in good condition
0326  E8 032F R                      call    write
0329  B0 00                         mov     al,0            ; so, quit with return code 0

032B  B4 4C                 Quit:   mov     ah,4Ch          ;function 4Ch of INT 21h
032D  CD 21                         int     21h             ; quit to system with return code in AL
032F                        SEARCH  endp


032F                        write   proc    near
032F  50                            push    ax
0330  B4 09                         mov     ah,9
0332  CD 21                         int     21h
0334  58                            pop     ax
0335  C3                            ret
0336                        write   endp


0336                        code    ends
                                    end     begin
```

รูปที่ 6 ขั้นตอนการคอมพายล์โปรแกรมเช็คขนาดของหน่วยความจำระบบ

```
C>a:masm search,,;
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987.  All rights reserved.


  51082 + 394006 Bytes symbol space free

      0 Warning Errors
      0 Severe  Errors

C>
C>a:link search;

Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

LINK : warning L4021: no stack segment

C>a:exe2bin search search.com

C>
```

PCTools หรือไม่งั้นก็จาก SideKick ก็ยังไหว (ตอนเริ่มเรียก SK จะมีรายงานขนาดของหน่วยความจำระบบอยู่ด้วย) แต่ไหน ๆ ก็ไหน ๆ แล้ว เรามาเขียนโปรแกรมเล็ก ๆ สักอันดีกว่า เพื่อเช็คตามเรื่องราวที่เราทราบมา โดยโปรแกรมจะไปอ่านขนาดหน่วยความจำระบบโดยตรงจาก BIOS Data Area เลย และจะทำการตรวจดูว่า มันเท่ากับ 633 กิโลไบต์มั้ย ถ้าใช่ก็แปลว่าเครื่องของคุณติดเชื้อเข้าให้แล้ว ก็จะแสดงผลออกมาดังรูปที่ 4 (ผมให้มาพร้อมกับ Op Code ดังรูปที่ 5) จากนั้นก็คอมพายล์ตามรูปที่ 6 ข้อดีของโปรแกรมตัวนี้เหนือ SI และ PCTools ก็คือมันเล็กกว่ามาก ก็เท่านั้น